REMARKS/ARGUMENTS

On the second page of the Detailed Action, the Examiner rejected claims 1,15, 24-32 and 38 under 35 U.S.C. § 102(e) as being anticipated by Peterka *et al.* (U.S. Patent Application Publication No. 2002/0170053 A1).

Before setting forth a discussion of the prior art applied in the Office Action, it is respectfully submitted that controlling case law has frequently addressed rejections under 35 U.S.C. § 102. "For a prior art reference to anticipate in terms of 35 U.S.C. Section 102, every element of the claimed invention must be identically shown in a single reference." *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 677, 7 U.S.P.Q.2d 1315, 1317 (Fed. Cir. 1988; emphasis added). If any claim, element, or step is absent from the reference that is being relied upon, there is no anticipation. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 230 U.S.P.Q. 81 (Fed. Cir. 1986; emphasis added). The following analysis of the present rejections is respectfully offered with guidance from the foregoing controlling case law decisions.

Applicant respectfully submits that Peterka *et al.* fails to teach or fairly suggest key limitations of the claims, and therefore Peterka *et al.* cannot be found to anticipate the present invention given the rulings in *Diversitech Corp. v. Century Steps, Inc.* and *Kloster Speedsteel AB v. Crucible, Inc.*

Peterka *et al.* describes a method for distributing encrypted data content which uses a hierarchy of encryption keys to provide for flexible billing options. Specifically, Peterka *et al.* describes a Pay-By-Time (PBT) billing option (See [0048]) in which a program is segmented into a plurality of program segments. The actual data of each respective program segment is then encrypted with at least one respective content key (CK). The respective content keys are then each encrypted with a respective program segment key (PSK). When a consumer wishes to join a multicast of the program, the consumer contacts an Origin Content Server (OCS) to begin receiving PSKs. The PSKs are distributed to the consumer in a multicast in which the PSKs are encrypted with the consumer's unique key (UK). In order to actually view a program segment, the consumer must first decrypt the PSK corresponding to that program segment with the consumer's UK, then use that decrypted PSK to decrypt the CK corresponding to that program

segment and then finally decrypt that program segment with the decrypted CK. In the Pay-By-Time billing method, the consumer must continue to request each new PSK in order to continue viewing the program, i.e. to continue decrypting program segments. Peterka also teaches that the content key for a future program segment may be encrypted with not only the PSK corresponding to the future program segment, but also with an old PSK of an old program segment. "Thus, if a user has not yet received a new program segment key, the content key can be obtained by utilizing the old program segment key." (see [0109] and Figure 9). Furthermore, Peterka *et al.* teaches that the content keys are maintained by the consumers, for possible use in later decryption. For example, Peterka describes a signalling method in which "a predetermined bit can be used to indicate **if an old or current content key should be used as opposed to a new content key** which has recently been distributed to the client." (see [0119]; emphasis added)

On pages 2 and 3 of the Detailed Action, the Examiner has alleged, in support of his rejection of claims 1, 15 and 38, that paragraphs [0080], [0082] and [0102] of Peterka *et al.* disclose the following feature of claims 1, 15 and 38:

> "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time."

Applicant respectfully disagrees and submits that Peterka *et al.* fails to teach or fairly suggest that decryption keys are delivered to a customer processing platform "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time", as recited in claims 1, 15 and 38. Paragraphs [0080], [0082] and [0102] of Peterka *et al.* merely recite that two PSKs are distributed at any given time; the current PSK corresponding to the current PS and the next PSK corresponding to the next PS. Peterka *et al.* does not recite any method or means for ensuring that the consumer has simultaneous possession of at most a subset of the plurality of decryption keys at any time. In fact, as described above, Peterka *et al.* specifically teaches that the content keys used to encrypt each PS are maintained by the consumer. For example, according to the teachings of Peterka, if a

consumer opts for the Pay-By-Time billing option and receives all of the program segments, and hence all of the PSKs and all of the CKs, the consumer would have a complete set of CKs, which the consumer could use to again view the encrypted content without requesting permission from the content provider.

Applicant also points out that at several points in the Detailed Action the Examiner has pointed to sections of Peterka *et al.* that recite details of program segment keys (PSK) when making reference to the decryption keys of the present invention. For example, as described above, the Examiner has pointed to paragraphs [0080], [0082] and [0102] of Peterka *et al.* in support of the rejection of claims 1, 15 and 38 on the ground that these paragraphs disclose the delivery of decryption keys according to claims 1, 15 and 38. Applicant submits that the program segment keys of Peterka *et al.* cannot be equated to either the encryption or decryption keys of the present invention, as the program segment keys of Peterka *et al.* are not used to encrypt data content, rather they are used to encrypt the content keys (CK) that are used to encrypt the data content.

In view of the fact that Peterka *et al.* fails to teach a key limitation of the claims, and also fails to identically show every element of the claimed invention, as is required to find that a prior art reference anticipates under 35 U.S.C. § 102, given the rulings in *Kloster Speedsteel AB v. Crucible, Inc.* and *Diversitech Corp. v. Century Steps, Inc.* respectively, the Examiner is respectfully requested to withdraw the 35 U.S.C. 102(e) rejection of claims 1, 15 and 38.

With regard to the Examiner's rejection of claims 24-32 under 35 U.S.C. § 102(e) as being anticipated by Peterka *et al.*, Applicant has cancelled claims 24-32.

On page 5 of the Detailed Action, the Examiner has rejected claims 35, 36 and 37 under 35 U.S.C. § 102(e) as being anticipated by Mourad *et al.* (U.S. Patent Application Publication No. 2006/0053077 A1). In response, Applicant has amended independent claims 35 and 37 such that amended independent claims 35 and 37 now recite in part:

> "first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a

customer computer system from a data content service provider system or another customer computer system; and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys, such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time".

Mourad *et al.* teaches a method and system for digital content distribution using web broadcasting services in which a customer purchases encrypted digital content from an electronic digital content store (see Figure 6). The customer registers with electronic digital content store in order to carry out a license purchasing transaction (See [0254]) and then receives the encrypted digital content either directly from the electronic digital content store or from a content hosting site. Once the license purchasing transaction is complete, the electronic digital content store authorizes a ClearingHouse to release the decryption keys for the encrypted digital content to the customer (see [0171]). In order to receive the decryption keys, the customer must request the decryption keys from the ClearingHouse. "When the ClearingHouse(s) 105 receives a request for a decryption key for the Content 113 from an intermediate or End-User(s), the ClearingHouse 105 validates the integrity and authenticity of the information in the request; verifies that the request was authorized by an Electronic Digital Store(s) or Content Provider(s) 101; and verifies that the requested usage complies with the content Usage Conditions as defined by the Content Provider(s) 101. Once these verifications are satisfied, the ClearingHouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s) packed in a License [secure container] SC" (see [0174]). The license control is designed with the ClearingHouse(s) as the "trusted party" (see [0255]). However, "[l]icence control requires that the Content Provider(s) 101, the Electronic Digital Content Store(s) 103, and the ClearingHouse(s) 105 have bona-fide

cryptographic digital certificates from reputable Certificate Authorities that are used to authenticate those components" (see [0257]).

Applicant respectfully submits that Mourad *et al.* fails to teach or fairly suggest key limitations of amended independent claims 35 and 37. Specifically, Mourad *et al.* fails to teach that data content encrypted in a plurality of sections with a corresponding plurality of encryption keys and that for each section of encrypted data content a corresponding one of a plurality of decryption keys is received and used to decrypt the encrypted section such that the processing platform carrying out the decryption has simultaneous possession of at most a subset of the plurality of decryption keys. Therefore, applicant submits that amended independent claims 35 and 37 distinguish over the teachings of Mourad *et al.* and dependent claim 36, which depends on claim 35, distinguishes for at least the same reasons.

On page 6 of the Detailed Action, the Examiner has rejected claims 2-13, 1-19, 21-23, 39 and 40-42 under 35 U.S.C. § 103(a) as being unpatentable over Peterka *et al.* in view of Stirling *et al.* (U.S. Patent Application Publication No. 2003/0223583 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a *prima facie* case of obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0080] of Stirling *et al.* in support of the rejection of claims 2-6 under 35 U.S.C. § 103(a). Paragraph [0080] of Stirling *et al.* recites a first layer of security in a secure data content delivery system, in which a key management and distribution system based on constructive key management. An architecture where the key is constructed from multiple components, tokens, keys and hardware. Paragraph [0080] of Stirling *et al.* refers to one such exemplary product available from TECSEC called Constructive Key Management (CKM) Software. The CKM software allows a Network Operations Center (NOC) to create authorization tokens for distribution to digital production facilities and intended exhibitor systems. Once the tokens are received at the clients, authorized users can encrypt or decrypt the digital content. The clients CKM software agents will construct (create) a key when needed for

encryption or decryption and destroy the key when no longer needed by the encryption/decryption engine.

Applicant submits that the Examiner has applied hindsight analysis in rejecting claim 2. Both Peterka *et al.* and Stirling *et al.* fail to teach or fairly suggest encrypting a plurality of sections of data content with a corresponding plurality of encryption keys and distributing decryption keys corresponding to the encryption keys to the processing platform of a consumer in a manner such that the consumer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys, as recited in independent claim 1. Dependent claim 2 depends on independent claim 1 and recites in part that a first decryption key is destroyed after a second decryption key is received, which is a specific mechanism of ensuring that the consumer processing platform has simultaneous possession of at most a subset, in this case two, of the plurality of decryption keys. Applicant submits that the Examiner is incorrect in equating the destroying of a decryption key when it is no longer needed by the decryption engine, as taught by Stirling *et al.*, with the destroying of a first decryption key at a customer processing platform after receiving a second decryption key, as recited in claim 2. There is no suggestion in Peterka *et al.* that any of the decryption content keys (CK) or program segment keys (PSK) are destroyed, let alone that any key is destroyed after a subsequent key is received. The suggestion in Stirling *et al.* that a decryption key is destroyed after a decryption engine is finished with it, is not sufficient to allow one skilled in the art to arrive at the subject matter of claim 2, namely that a first decryption key is destroyed after a second decryption key is received.

It should be further noted that according to the teachings of Peterka *et al.*, content keys (CK) are distributed to consumers in an encrypted form. The encrypted form must be decrypted using at least one of the keys higher in the encryption hierarchy. For example, in the Pay-By-Time billing method, a message is received by the consumer, which must be first decrypted with a unique key (UK) to recover a PSK and the PSK must then be used to recover the CK. Even if the CK is destroyed, the consumer could recover it by simply decrypting the message again with the UK and the PSK. Therefore, destroying a CK according to the teachings of Peterka *et al.* in view of the teachings of Stirling *et al.* would be insufficient to "ensure that content is only used

for the number of times permitted", which the Examiner has suggested is the motivation for combining these two references.

With regard to the Examiner's rejection of claims 3 to 6, the Examiner has relied upon the same paragraph in Stirling *et al.*, namely paragraph [0080], in rejecting claims 3 to 6 as was relied upon in the rejection of claim 2. Each of the arguments presented in response to the Examiner's rejection of claim 2 are equally applicable to the Examiner's rejection of claims 3 to 6. Applicant submits that claims 3 to 6 distinguish over the teachings of Peterka *et al.* and Stirling *et al.* alone and in combination for at least the same reasons as claim 2.

With regard to the Examiner's rejection of claim 7, the Examiner has pointed to Figures 8 and 9 of Peterka *et al.* in support of the rejection of claim 7. Figures 8 and 9 of Peterka *et al.* illustrate encrypted data content distribution methods that include: receiving a request for a cryptographic key from a client; logging the request for the key; logging a segment of the program content for which the key can be used; distributing one or more decryption keys; **distributing program content for decryption by the client utilizing the key; and billing the client based upon log entry(ies).** Therefore, according to Figures 8 and 9 of Peterka *et al.*, and Peterka *et al.* as a whole, a client must request the cryptographic key and download the program content again each time the client wishes to use the data content. According to the teachings of Peterka *et al.*, the client is only billed once the client has re-downloaded the key and the program content, which is completely different than the billing mechanism recited in claim 7. Claim 7 recites:

> "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform".

Therefore, claim 7 clearly recites that the client is billed for the delivery of the encrypted sections and is then billed for each use of the data content.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 7, as the cited reference fails to teach all of the claimed limitations of claim 7.

With regard to the Examiner's rejection of claims 8 and 9, the Examiner has relied solely on a portion of Peterka *et al.* in supporting the rejection of claims 8 and 9. Applicant submits that claims 8 and 9 depend from claim 1, which as demonstrated above, distinguishes over the teachings of Peterka *et al.* Therefore, Applicant submits that claims 8 and 9 distinguish over the teachings of Peterka *et al.* for at least the same reasons as claim 1.

With regard to the Examiner's rejection of claim 10, the Examiner has pointed to paragraphs [0097], [0114] and [0124] of Peterka *et al.* in support of the rejection of claim 10. Paragraphs [0097], [0114] and [0124] of Peterka *et al.* recite the encryption of a first key with a second key that is higher in a key hierarchy than the first key. For example, the encryption of a content key (CK), which is used to encrypt data content, with a program segment key (PSK). Claim 10 recites:

> "**generating** each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby **generate** a plurality of customer processing-specific keys" (emphasis added).

The "pluralilty of encryption keys" recited in claim 10 refer to the plurality of encryption keys that are used to encrypt the plurality of sections of data content. According to the teachings of Peterka *et al.*, the content keys (CK) are used to encrypt sections of data content (see [0103]). As indicated above, Peterka *et al.* discloses that the content keys may be **encrypted** with a higher level key, i.e. a unique key, program segment key, etc., but Peterka *et al.* fails to teach or fairly suggest that the encryption key used to encrypt the section of data content, i.e. the content keys (CK), are **generated** "using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing-specific keys", as recited in claim 10.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 10, as the cited reference fails to teach all of the claimed limitations of claim 10.

With regard to the Examiner's rejection of claim 11, the Examiner has pointed to paragraphs [0097], [0114] and [0124] and claim 23 of Peterka *et al.* in support of the rejection of claim 11. As describe above, paragraphs [0097], [0114] and [0124] of Peterka *et al.* recite the

encryption of a first key with a second key that is higher in a key hierarchy than the first key. Claim 23 of Peterka *et al.* also relates to encrypting a first key with a second key that is higher in the key hierarchy than the first key. Claim 11 recites:

> "wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value".

Claim 11 depends on claim 10 and distinguishes over the teachings of Peterka *et al.* for at least the same reasons as claim 10. However, claim 11 also recites additional limitations that are not disclosed by Peterka *et al.* Specifically, Peterka *et al.* fails to teach or fairly suggest that each encryption key is generated using an identifier associated with a customer processing platform and a respective key generation seed value.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 11, as the cited reference fails to teach all of the claimed limitations of claim 11.

With regard to the Examiner's rejection of claim 12, the Examiner has relied upon the same portions of Peterka *et al.*, namely paragraphs [0097], [0114] and [0124] and claim 23, in support of the rejection of claim 12 as were relied upon in the rejection of claim 11. Applicant submits that claim 12 depends on claim 11 and distinguishes for at least the same reasons as claim 11. Furthermore, Applicant submits that claim 12 recites additional limitations that are not disclosed by Peterka *et al.* Specifically, as described above, Peterka *et al.* fails to disclose that the encryption keys are generated using an identifier associated with a customer processing platform and a respective key generation seed value, and therefore Peterka *et al.* certainly fails to teach or fairly suggest that "delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values", as recited in claim 12.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 12, as the cited reference fails to teach all of the claimed limitations of claim 12.

With regard to the Examiner's rejection of claim 13, Applicant submits that claim 13 depends on claim 1 and therefore distinguishes over the teachings of Peterka *et al.* for at least the same reasons as claim 1, as provided above.

With regard to the Examiner's rejection of claims 16 and 21, the Examiner has relied upon the same portion of Stirling *et al.*, namely paragraph [0080], in support of the rejection of claims 16 and 21 as was relied upon in the rejection of claims 2 to 6. Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claims 16 and 21. Furthermore, paragraph [0080] of Stirling *et al.* merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine.** This recitation by Stirling *et al.* does not recite "destroying the decryption key **after completing playback of the encrypted section**" (emphasis added), as recited in claims 16 and 21. As described above, Peterka *et al.* is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka *et al.* and Stirling *et al.* would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claims 16 and 21, as the cited references fail to teach all of the claimed limitations of claims 16 and 21.

With regard to the rejection of claim 17, the Examiner has once again relied on paragraph [0080] of Stirling *et al.* in the rejection of claim 17. As described above, paragraph [0080] of Stirling *et al.* relates to the creation of **a decryption key** when necessary and the destroying of **the decryption key** when no longer needed by the decryption engine. Applicant submits that paragraph [0080] of Stirling *et al.*, and Stirling *et al.* as a whole, does not teach or fairly suggest "destroying **decrypted data content** at the customer processing platform **after completing playback of the encrypted section**" (emphasis added), as recited in claim 17.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 17, as the cited references fail to teach all of the claimed limitations of claim 17.

With regard to the rejection of claims 18 and 19, Applicant submits that claims 18 and 19 depend on claim 16 and therefore distinguish over the teachings of Peterka *et al.* and Stirling *et al.*, alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 22, similar to the rejection of claims 10, 11 and 12, the Examiner has mistakenly relied upon the recitation in Peterka *et al.* that a encryption key, i.e. a content key (CK), may be encrypted with a key higher in the key hierarchy, i.e. a unique key (UK), for the purposes of multicast transmission, in rejecting claim 22. Claim 22 recites that "each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform". Applicant submits that encrypting a content key for the purposes of multicast transmission is completely different than encrypting the plurality of sections of data content with a plurality of customer processing platform-specific keys which are determined based on an IP address of the customer processing platform.

According to the teachings of Peterka *et al.*, the encrypted content keys are decrypted with the higher level key, i.e. the unique key (UK), and the content keys are then used to decrypt the corresponding program segments. Once the content key is decrypted with the higher level key, it is completely untraceable, as any customer specific information has been stripped during the decryption of the content key. In contrast, the method according to claim 22 provides for traceability of the decryption key and the encrypted data content, because the sections of data content are encrypted with customer processing platform-specific keys.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 22, as the cited references fail to teach all of the claimed limitations of claim 22.

With regard to the rejection of claim 23, Applicant submits that claim 23 depends on claim 16 and therefore distinguish over the teachings of Peterka *et al.* and Stirling *et al.*, alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 39, similar to the Examiner's rejection of claims 16 and 21, Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claim 39. Furthermore, the Examiner has once

again relied on paragraph [0080] of Stirling *et al.*, which as described above merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine**. This recitation by Stirling *et al.* does not recite "means for destroying the decryption key, **after completing playback of the encrypted section**" (emphasis added), as recited in claim 39. As described above, Peterka *et al.* is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka *et al.* and Stirling *et al.* would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 39, as the cited references fail to teach all of the claimed limitations of claim 39.

With regard to the rejection of claim 40, the Examiner has pointed to paragraph [0047] of Stirling *et al.* in support of the rejection of claim 40. Paragraph [0047] of Stirling *et al.* recites:

> "The distribution entity 106 includes **a conditional access management system** (CAMS) 132 (also referred to as a configuration management engine), that accepts the output media content data 128, and **determines whether access permissions are appropriate** for the content data 128. Further, **CAMS 132 may be responsible for additional encrypting** so that unauthorized access during transmission is prevented. Once the data is in the appropriate format and access permissions have been validated, **CAMS 132 provides the output media content data 128 to an uplink server 134**, ultimately for transmission by uplink equipment 136 to one or more displaying entities" (emphasis added).

It is clear that paragraph [0047] of Stirling *et al.* is not directed to processing a permission request that is separate from a download request, such that the permission request grants permission to use the downloaded content, but rather is directed to a conditional access management system (CAMS) that determines whether a download request should be granted, and if so "provides the output media content data 128 to an uplink server 134" so that a display entity may download the media content data. Therefore, the access permissions of Stirling *et al.* cannot be equated to the permission requests recited in claim 40. Applicant submits that Peterka *et al.* and Stirling *et al.*, alone or in combination, fail to teach or fairly suggest a data content server

configured to "transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content", and a data content download controller configured to "generate permission requests when downloaded data content is to be used", as recited in claim 40.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 40, as the cited references fail to teach all of the claimed limitations of claim 40.

With regard to the rejection of claims 41 and 42, Applicant submits that claims 41 and 42 depend on claim 40 and therefore distinguish over the teachings of Peterka *et al.* and Stirling *et al.*, alone or in combination, for at least the same reasons as claim 40, as provided above.

In view of the foregoing, Applicant respectfully submits that a *prima facie* case of obviousness cannot be established against claims 2-13, 16-19, 21-23, 39 and 40-42 as one or more key limitations of each of the claims is missing from both of the cited references. Applicant respectfully submits that claims 2-13, 16-19, 21-23, 39 and 40-42 are patentable over Peterka *et al.* and Stirling *et al.* since a *prima facie* case of obviousness cannot be established.

On page 17 of the Detailed Action, the Examiner has rejected claims 14 and 33 under 35 U.S.C. § 103(a) as being unpatentable over Peterka *et al.* in view of Ginter *et al.* (U.S. Patent Application Publication No. 2006/0218651 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a *prima facie* case of obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

With regard to the rejection of claim 14, Applicant submits that claim 14 depends on claim 1 and therefore distinguishes over the teachings of Peterka *et al.* for at least the same reasons as claim 1, namely that Peterka *et al.* fails to teach or fairly suggest that decryption keys are delivered "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption at any time".

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 14, as the cited references fail to teach all of the claimed limitations of claim 14.

With regard to the rejection of claim 33, in response Applicant has cancelled claim 33.

On page 18 of the Detailed Action, the Examiner has rejected claims 20 and 43 under 35 U.S.C. § 103(a) as being unpatentable over Peterka *et al.* in view of Stirling *et al.* and further in view of Ginter *et al.*

To begin, Applicant respectfully submits that a first criterion required to establish a *prima facie* case of obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

Claims 20 and 43 depend on claims 16 and 40 respectively. In view of the arguments presented above regarding the Examiner's rejection of claims 16 and 40, Applicant submits that Peterka *et al.* and Stirling *et al.* fail to teach or fairly suggest key limitations of claims 16 and 40 and hence of claims 20 and 43. Applicant submits that Ginter *et al.* similarly fails to teach or fairly suggest these key limitations and therefore claims 20 and 43 distinguish over the teachings of Peterka *et al.*, Stirling *et al.* and Ginter *et al.* both alone and in combination.

On page 19 of the Detailed Action, the Examiner has rejected claim 34 under 35 U.S.C. § 103(a) as being unpatentable over Peterka *et al.* in view of Negawa (U.S. Patent Application Publication No. 2003/0046539 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a *prima facie* case of obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0078] of Negawa in support of the rejection of claim 34, alleging that this paragraph teaches "a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. Applicant submits that Negawa recites "a multicast communication system having a multicast server and a plurality of clients belonging to a multicast group. The multicast server

transmits data encrypted by using a first encryption key to the clients by multicasting, and **transmits the results of encrypting the first encryption key by using a second encryption key** by unicasting to a client subscribed to a data distribution service, among the plurality of clients. The client subscribed to the data distribution service receives the encrypted data and the result. **The client decrypts the result to obtain the first encryption key and decrypts the encrypted data using the first encryption key"** (see Abstract; emphasis added). According to the teachings of Negawa, a client device plugs into a distribution data receiving device (see Figure 4) in order to receive encrypted data content and decryption keys from a content server (see Figure 2). The distribution data receiving device includes a key decryption key holding unit 34 that holds a key decryption key Km. Key decryption key Km is the "second encryption key" that is used to encrypt the "first encryption key", which is called the group decryption key Kgr. "Key decryption key Km is preferably stored (formed) in key decryption key holding unit 34 in the form of a hardware circuit (for example an IC chip) to ensure that key decryption key Km cannot easily be read by a third party" (see [0058]).

Paragraph [0078] of Negawa recites that "[w]hen control unit 30 **receives a withdrawal request** from client 3c, it deletes (or destroys) the key decryption key Km(C) held in key decryption key holding unit 34 and deletes (or destroys) the group session key Kgr held in key decryption unit 33". In other words, when the client 3c no longer wishes to decrypt further data content, i.e. the client 3c issues a withdrawal request, the control unit 30 destroys or deletes the key decryption key Km(C) and the group session key Kgr. This is completely different than "for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. For example, according to Negawa, the key decryption key Km is needed to decrypt the unicast message containing the session key Kgr. If the key decryption key Km is deleted or destroyed then there would be no point in "transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data" as the customer data content processing device would be unable to decrypt the "different key" in order to decrypt the "subsequent portion of the encrypted data".

In addition, not only does Negawa fail to teach or fairly suggest the particular feature that the Examiner alleges, but modifying the method of Peterka *et al.* by incorporating the method of key deletion according to Negawa would render Peterka *et al.* unsuitable for its intended purpose. Peterka *et al.* teaches a hierarchy of encryption keys for multicast distribution of encrypted digital content. According to Peterka *et al.* a content key (CK) is used to encrypt a section of digital content and the content key (CK) is then encrypted with one or more keys that are higher in the key hierarchy than the encryption key. For example, the content key (CK) may be encrypted with a program segment key (PSK) that is in turn encrypted with a unique key (UK) that is unique to a consumer and allows the consumer to decrypt the PSK and hence the CK. If the unique key (UK) of the consumer's processing platform is deleted, the consumer would be only unable to decrypt the PSK and hence the CK for subsequent content segments, but would also cause the consumer to be unable to request subsequent PSKs, due to the fact that the UK is required to "initiate the key request message exchange with a particular caching server" (see [0097] of Peterka *et al.*). If the UK is deleted, the customer would have to re-register with the content provider in order to receive a new UK, which would render the teachings of Peterka *et al.* unsuitable for its intended purpose.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 34, as the cited references fail to teach all of the claimed limitations of claim 34 and the incorporation of the subject matter of Negawa would render the operation of Peterka *et al.* unsuitable for its intended purpose.

In view of the forgoing, early favorable consideration of this application is earnestly solicited. In the event that the Examiner has concerns regarding the present response the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

SO, VINCENT

By _____
Allan Brett
Reg. No. 40,476
Tel.: (613) 232-2486 ext. 323

Date: January 24, 2007

RAB:JFS:mcg